(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平7－271884

(43)公開日　平成７年(1995)10月20日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　19/00				
Ｇ０９Ｃ　1/00		9364－5L		
Ｈ０４Ｌ　9/00				
			Ｇ０６Ｆ　15/ 30　３４０	
			３６０	

審査請求　未請求　請求項の数12　ＦＤ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平7－49237

(22)出願日　平成７年(1995)２月15日

(31)優先権主張番号　１９８８００

(32)優先日　1994年２月17日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390035493
エイ・ティ・アンド・ティ・コーポレーション
ＡＴ＆Ｔ　ＣＯＲＰ.
アメリカ合衆国　10013－2412　ニューヨーク　ニューヨーク　アヴェニュー　オブ　ジ　アメリカズ　32

(72)発明者　マイケル　ジョン　メリット
アメリカ合衆国、60563　イリノイ、ネイパービル、＃1329、イロクオイス　アベニュー　1101

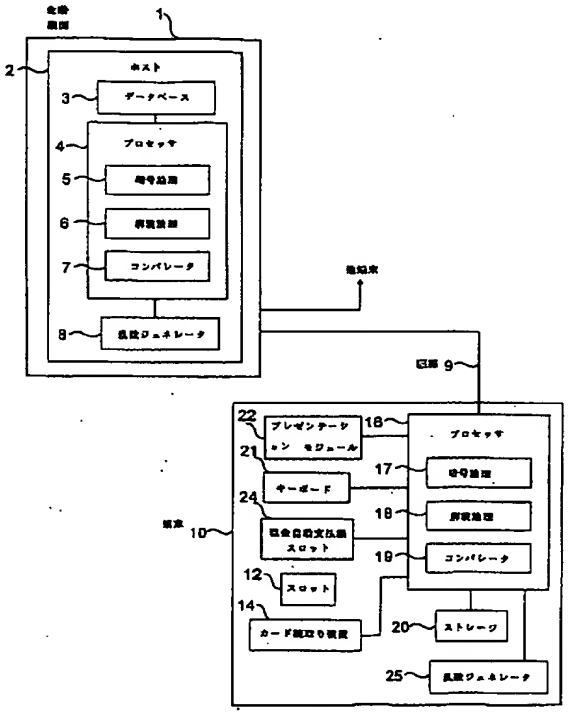
(74)代理人　弁理士　三俣　弘文

(54)【発明の名称】　端末認証方法

(57)【要約】

【目的】　トランザクション実行システムで自動窓口端末機のような端末をユーザつまり顧客に対し認証する対顧客端末認証法を提供する。

【構成】　この端末は暗号方式を用い中央ホストにより認証されるが、パーソナル・セキュリティ・フレーズ（ＰＳＰ）がこの端末からそのホストへ送信される。このＰＳＰを組込んだメッセージをこの端末によりその顧客へ通信されそれによりこの端末が正当であることを示す。この顧客がパーソナル識別番号のような何らかの秘密情報をこの端末に入力する前にこの端末をこの顧客に対し認証する。



1

【特許請求の範囲】

【請求項１】　トランザクション実行システムでユーザに対し端末を認証する端末認証方法において、

（Ａ）前記端末に口座情報を受信する口座情報受信ステップと、

（Ｂ）前記口座情報を発行した機関と関係付けられたホストと通信回線を経て接触する接触ステップと、

（Ｃ）前記端末から前記ホストへ前記口座情報の少なくとも一部を送信する口座情報送信ステップと、

（Ｄ）　前記ホストから前記端末へ前記口座に対応したパーソナル・セキュリティ・フレーズを送信するパーソナル・セキュリティ・フレーズ送信ステップと、

（Ｅ）前記端末において前記ユーザに対し前記パーソナル・セキュリティ・フレーズを組込んだメッセージを通信する通信ステップと、を有し、前記ステップは前記端末に前記ユーザがいずれかの秘密または機密の情報を入力するステップに先だって行うことを特徴とする端末認証方法。

【請求項２】　前記（Ｅ）ステップは、前記端末に結合したプレゼンテーション・モジュールに前記パーソナル・セキュリティ・フレーズを表示する表示ステップを有することを特徴とする請求項１に記載の方法。

【請求項３】　前記（Ｄ）ステップは、複数の英数字、複数のワード、ビデオ画像、ビデオ画像のシーケンスのいずれかの形を持つパーソナル・セキュリティ・フレーズを送信するステップを有することを特徴とする請求項２に記載の方法。

【請求項４】（Ｆ）前記パーソナル・セキュリティ・フレーズ送信ステップは録音の形を持つパーソナル・セキュリティ・フレーズを送信するステップと、

（Ｇ）前記パーソナル・セキュリティ・フレーズを組込んだメッセージを通信する前記通信ステップは前記端末に結合したプレゼンテーション・モジュールを経て前記パーソナル・セキュリティ・フレーズを音声で送信するステップとを更に有することを特徴とする請求項１に記載の方法。

【請求項５】　前記端末は自動窓口端末機であることを特徴とする請求項１に記載の方法。

【請求項６】　前記ステップは前記自動窓口端末機にパーソナル識別番号を前記ユーザが入力するステップに先だって行うことを特徴とする請求項５に記載の方法。

【請求項７】　前記（Ｅ）ステップは、さらに、前記ユーザが前記パーソナル・セキュリティ・フレーズを前記ユーザ自身のものと認める場合にのみ前記自動窓口端末機に前記ユーザのパーソナル識別番号を入力するよう前記ユーザに命令する命令ステップを有することを特徴とする請求項６に記載の方法。

【請求項８】　さらに、（Ｈ）前記端末を前記ホストに対し認証する端末認証ステップを有し、前記（Ｈ）ステップは、前記（Ｄ）ステップに先だって行うことを特徴

2

とする請求項１に記載の方法。

【請求項９】　前記（Ｅ）ステップは、前記端末に結合したプレゼンテーション・モジュールで前記パーソナル・セキュリティ・フレーズを表示するステップを有することを特徴とする請求項８に記載の方法。

【請求項１０】　前記（Ｄ）ステップは、複数の英数字、複数のワード、ビデオ画像、ビデオ画像のシーケンスのいずれかの形を持つパーソナル・セキュリティ・フレーズを送信するステップを有することを特徴とする請求項９に記載の方法。

【請求項１１】　前記（Ｈ）ステップは、

（Ｈ１）前記自動窓口端末機と関係付けられた通し番号を前記ホストに送信する通し番号送信ステップと、

（Ｈ２）前記ホストにおいて第１の乱数を生成する第１の乱数生成ステップと、

（Ｈ３）前記第１の乱数を前記ホストから前記自動窓口端末機へ送信する第１の乱数送信ステップと、

（Ｈ４）前記自動窓口端末機に蓄積した安全保障の第１のキーを用いて、前記通し番号と前記第１の乱数と第１の指示コードの暗号を前記自動窓口端末機において計算する第１のキー使用暗号計算ステップと、

（Ｈ５）前記自動窓口端末機から前記ホストへ安全保障の前記第１のキーを用いて前記通し番号と前記第１の乱数と前記第１の指示コードの前記暗号を送信する暗号送信ステップと、

（Ｈ６）前記ホストに蓄積した安全保障の第２のキーを用いて前記通し番号と前記第１の乱数と前記第１の指示コードの暗号を前記ホストにおいて計算する第２のキー使用暗号計算ステップと、

（Ｈ７）前記第２のキーを用いて計算した前記通し番号と前記第１の乱数と前記第１の指示コードの前記暗号と、前記第１のキーを用いて計算した前記通し番号と前記第１の乱数と前記第１の指示コードの前記暗号を、前記ホストにおいて比較する暗号比較ステップと、

（Ｈ８）前記第２のキーを用いて計算した前記通し番号と前記第１の乱数と前記第１の指示コードの前記暗号と、前記第１のキーを用いて計算した前記通し番号と前記第１の乱数と前記第１の指示コードの前記暗号が等しいことを、前記ホストにおいて検証する検証ステップを有すること特徴とする請求項８に記載の方法。

【請求項１２】　前記（Ｈ）ステップは、

（Ｈ１）前記自動窓口端末機において第２の乱数を生成する第２の乱数生成ステップと、

（Ｈ２）前記第２の乱数を前記自動窓口端末機から前記ホストへ送信する第２の乱数送信ステップと、

（Ｈ３）前記第１のキーを用いて前記通し番号と前記第２の乱数と前記第１の指示コードと異なる第２の指示コードの暗号を前記ホストにおいて計算する第１のキー使用暗号計算ステップと、

（Ｈ４）前記ホストから前記自動窓口端末機へ前記第１

のキーを用いて前記通し番号と前記第２の乱数と前記第２の指示コードの暗号を送信する暗号送信ステップと、

（Ｈ５）前記第２のキーを用いて前記通し番号と前記第２の乱数と前記第２の指示コードの暗号を前記自動窓口端末機において計算する第２のキー使用暗号計算ステップと、

（Ｈ６）前記第２のキーを用いて計算した前記通し番号と前記第２の乱数と前記第２の指示コードの前記暗号と、前記第１のキーを用いて計算した前記通し番号と前記第２の乱数と前記第２の指示コードの前記暗号を、前記自動窓口端末機において比較する暗号比較ステップと、

（Ｈ７）前記第２のキーを用いて計算した前記通し番号と前記第２の乱数と前記第２の指示コードの前記暗号と、前記第１のキーを用いて計算した前記通し番号と前記第２の乱数と前記第２の指示コードの前記暗号が、等しいことを前記自動窓口端末機において検証する検証ステップとを更に有することを特徴とする請求項８に記載の方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、トランザクション実行システムに係り、特にこのトランザクション実行システムには中央ホストがあって取引処理、例えば、現金の払出または口座間預金振替のようなトランザクションを実行できる遠隔端末と通信しトランザクションを実行するトランザクション実行システムの要素をユーザつまり顧客に対し認証する認証方法に関する。

【０００２】

【従来の技術】トランザクション端末、例えば、何時でも動作可能な自動窓口端末機（ＡＴＭ）は、無人場所で現金の払出や他の金融取引処理のトランザクションの要望を満たすためこの利用は広く受入れられてきた。ＡＴＭの便利なことからこのような処理は一般大衆に非常に普及した。さらに、小売商品販売店のオーナが知ったことというのは、ＡＴＭの見込める場所は顧客をその小売場所に引寄せ顧客が現金購入するという件数が増加したことである。そのためＡＴＭ場所は銀行のような関連金融機関の場所から遠く離れた場所である場合が多い。このようなＡＴＭや他のトランザクション端末の分布システムからいくつかの複雑なセキュリティ問題が生じた。この金融業界は特にこのセキュリティ問題に関心を持っている。

【０００３】ＡＴＭを用いる、例えば、電子預金振替（ＥＦＴ）システムでは、トランザクションを実行するために機器上でそのユーザの署名、ただしこれは容易に偽造可能であるが、これを通常必要としない。それより、そのユーザの秘密のパーソナル識別番号（ＰＩＮ）とプラスチックの銀行カードつまりトランザクション・カードがこのＥＦＴシステムに対しそのユーザを識別し

検証するための役目をする。このＰＩＮは、例えば、４桁の番号でできる。通常はこのユーザがその銀行カードをこのＡＴＭのスロットに挿入しその後このＡＴＭがそのユーザにユーザのＰＩＮの入力をプロンプトする。次にこのユーザはそのＰＩＮをそのＡＴＭに付随するキーボードに入力すると、このＡＴＭは次にそのＰＩＮをこのＡＴＭに結合したデータベースの蓄積情報と比較する。

【０００４】この比較で適切なＰＩＮが入力されたことを示す場合にのみそのトランザクションは進むことができる。いくつかのセキュリティ問題は、正当な顧客のＰＩＮや他の口座情報を得た不正者の場合に生ずる。この状況に特に関心が払われる理由は、この不正者がその正当な顧客の専用口座の蓄積情報にアクセスできまたその口座の蓄積預金にアクセスできるからである。この問題に対応して、この金融業界はＰＩＮ番号と銀行カードの不正使用に対抗するためいろいろな方法を適用してきた。例えば、このユーザがそのＰＩＮをそのＡＴＭに付随のキーボードに入力してしまうとそのＰＩＮを符号化するため暗号動作を使用することが知られている。このような対抗法により不正者がネットワーク・リンクで送られるメッセージをモニタしたりそのためＰＩＮ情報を入手したりできぬようにする。

【０００５】ところが最近、ＰＩＮや他の口座情報を入手するため不正者は高度で精巧な方法を使用するようになってきた。このような不正な方法の一例に偽造ＡＴＭを商店街や他の公共の場所に設置する例がある。この偽造端末機は、顧客がその銀行カードつまりトランザクション・カードを挿入しそのＰＩＮを入力しても現金の払出はしない。しかし、この偽造端末機は、この端末機で行われた現金払出の無効な試行でその顧客が入力したカード口座番号やＰＩＮを保持し記録する。そしてこの記録情報を用いて実際の銀行カードのアクションを活動化する偽造プラスチック・カードの作成を可能にする。その偽造端末機が記録したＰＩＮと共にこの偽造カードを正当なＡＴＭで用いて他人の銀行口座の蓄積預金の振替または引出が可能となる。

【０００６】以上説明した例のようなスキームからＡＴＭまたは他のトランザクション端末をユーザまたは顧客に対し認証する認証法が必要で、それも秘密または機密の情報をそのＡＴＭまたは他のトランザクション端末にそのユーザまたは顧客が提供する前に、認証法が必要である。通信システムにおいて暗号方式を用いてハードウェア要素を互いに認証する認証方法は既知である。この認証方法の一例に、米国特許第４，７９９，０６１号、“安全保障要素認証システム”、アブラハム＝（Ａｂｒａｈａｍ）ら、に開示の方法を挙げることができる。しかしこれらの方法は、その要素をユーザつまり顧客に対して認証しない。ユーザに機密情報を入力するよう要求する端末をユーザに対し認証する問題は以前にも認めら

5

れており、いくつかの参考文献の中に下記のような解決法の一例が知られている。

【０００７】それは、別個のパーソナル・ポータブル端末デバイスをそのユーザに提供する方法である。米国特許第４、５２９、８７０号、“暗号識別、金融トランザクションおよび信用証明デバイス”では、例えば、次のような暗号装置を提供する。この暗号装置は、外部コンピュータ・システムに対しその身元を明らかにするためその所有者により使用され、そして外部システムと種々の金融トランザクションを実行でき、また外部システムに対し種々の信用証明を提供できる。一実施例では、この装置は、暗号デバイスとパーソナル端末デバイスに分離可能である。この装置の所有者はそのパーソナル端末デバイスをおそらくよく制御し、機密データが業者の販売時点端末のような端末に不当に保持されないようにする。しかし、このようなデバイスにも追加ハードウェアをそのカード形状デバイスに組込む必要がありまたこのデバイスや他のシステム要素が通信できるよう追加変更が必要である。

【０００８】

【発明の解決しようとする課題】このような追加や変更の必要の無い自動窓口端末機のような端末をユーザつまり顧客に対し認証する有効な対顧客端末認証法が要望されている。

【０００９】

【課題を解決するための手段】本発明は、トランザクション実行システムに以下に説明する認証方法を提供し前記課題を解決しこの分野の技術的進歩を遂げる。すなはち本発明は、トランザクション実行システムには中央ホストがあって、例えば、現金の払出または口座間預金振替のトランザクションを実行できる遠隔端末と通信しトランザクションを実行するシステムの要素をユーザつまり顧客に対し認証する認証方法を提供する。本発明の認証方法には次のステップがある。すなわち、端末において口座情報を受信する口座情報受信ステップと、前記口座情報を発行した機関に関係付けられたホストと通信回線を経て接触する接触ステップと、前記端末から前記ホストへ前記口座情報の少なくとも一部を送信する送信ステップと、前記ホストから前記端末へ前記口座に対応するパーソナル・セキュリティ・フレーズを送信するパーソナル・セキュリティ・フレーズ送信ステップがある。

【００１０】さらに本発明の認証方法には、前記端末において前記ユーザに対し前記パーソナル・セキュリティ・フレーズを組込んだメッセージを通信する通信ステップがある。さらに本発明の方法では、前記ステップは前記ユーザがいずれかの秘密または機密の情報を入力するステップに先だって生ずるものである。さらに本発明の認証方法の特徴と利点は以下の詳細な説明と添付参照図面から明白である。

【００１１】

6

【実施例】図１は本発明に特に好都合なトランザクション実行システムを示す図である。機関１は例えば、銀行のような金融機関である。この銀行１にはホスト２がある。このホスト２にはデータベース３とプロセッサ４がある。このプロセッサ４には暗号論理５と解読論理６とコンパレータ７がある。またこのホスト２には乱数ジェネレータ８がある。端末１０は、例えば複数の地理的に分布した自動窓口端末機（ＡＴＭ）の中の１個のＡＴＭである。このＡＴＭは例えば電話回線のような通信回線９によりその銀行のホスト２に結合する。このＡＴＭ１０には、顧客が挿入した銀行カードを受入れたり戻したりするスロット１２があり、さらにこのカードに蓄積した情報を読取る手段のカード読取り装置１４がある。

【００１２】このカード読取り手段１４はプロセッサ１６に結合する。このプロセッサ１６には暗号論理１７と解読論理１８とコンパレータ１９がある。乱数ジェネレータ２５もまたこのプロセッサ１６に結合する。またこのＡＴＭ１０には情報またはデータを蓄積する手段のストレージ２０があり、このストレージ２０はプロセッサ１６に結合する。さらにこのＡＴＭ１０にはまたキーボード２１とプレゼンテーション・モジュール２２があり、これらはプロセッサ１６に結合する。このプレゼンテーション・モジュール２２には例えば、次のような表示手段のある表示画面を挙げることができる。この表示手段は静止画像または画像シーケンス、例えば、ビデオ画面をビデオ・カードで表示する手段である。このプレゼンテーション・モジュール２２にはまた音声通信手段があり、これは音声カードで例えば、スピーカのように音声を通信する手段である。

【００１３】最後にこのＡＴＭ１０には現金を自動支払する第２のスロット２４があり、これもまたプロセッサ１６に結合する。さらに図１には図示していないが、この銀行ホスト２に結合できる追加端末がある。このＡＴＭ１０のような新規端末が図１に示すトランザクション実行システムの一部としてオンライン状態に入ると、この銀行１はそれに通し番号のＳと暗号キーのＫを割当てる。この通し番号のＳは例えば、４桁または他の適当な長さの番号とすることができる。この暗号キーのＫは安全保障暗号スキームに使用できるものである。Ｋには例えば、５６ビット・データ暗号規格（ＤＥＳ）キーを挙げることができ、これは例えば、“データ暗号規格”、ＦＩＰＳ、Ｐｕｂ．４６、米国標準規格局（１９７７年１月）、に記載のような暗号システムに使用のものである。

【００１４】ここに参照する前記報告、関連報告および特許を引例とし説明を続ける。この通し番号と暗号キーはそのＡＴＭストレージ手段２０と銀行ホスト２の両者に蓄積される。この銀行１で顧客が口座を得るよう登録するとこの顧客に口座番号が割当てられる。この銀行１はこの顧客にプラスチックのトランザクション・カード

すなわち銀行カードを通常供与するが、このカードには適当な口座情報を含む磁気ストリップがある。この情報にはこのカードを発行した銀行を識別する銀行識別番号とこの顧客の口座番号と顧客名を通常含むが、他の情報もまた含むことができる。（このトランザクション・カードにはまた例えば、米国特許第４、７９５、８９８号に記載のようなスマート・カードを挙げることができる。）次にこの顧客は例えば、４桁番号のパーソナル識別番号（ＰＩＮ）を選択しまたはこの顧客にそれが割当てられる。

【００１５】このＰＩＮは機密が保持されこのカードの使用許可の無い者にはそれを伝えないよう一般に意図されている。本発明の方法ではこの顧客はまたパーソナル・セキュリティ・フレーズ（ＰＳＰ）を選択しまたはこの顧客にそれが割当てられる。このパーソナル・セキュリティ・フレーズにはワードつまり英数字のいずれかの組合わせを用いることができるが、その全体の長さは所定の長さ以下でその特定の顧客が比較的記憶または認識し易いフレーズが好ましい。ただしこのＰＳＰは英数字に限定するものではない。このＰＳＰは電子的に伝送可能な静止画または画像シーケンスでもよい。同様にこのＰＳＰは録音音声の形でもよい。英数字のある組合わせの形を取るＰＳＰの場合と同様にビデオＰＳＰまたは音声ＰＳＰもその顧客が比較的記憶または認識し易いものが好ましい。

【００１６】次にこのＰＳＰは他の情報と共にこの銀行１の係員によりそのホスト２に入力されるが、この他の情報にはその顧客名やその顧客の口座番号やその顧客のＰＩＮがある。このＰＩＮそれ自身はそのホスト２に蓄積されず、むしろこのＰＩＮの暗号化バージョンやまたはハッシュ・バージョンを例えば、ワンウェイ・ファンクションを用いて蓄積する。このワンウェイ・ファンクションは従来周知であり、これについては例えば、次に挙げる報告に記載があり参照のこと。エイ・エバンス（Ａ．Ｅｖａｎｓ）ら、“コンピュータにおける秘密不要ユーザ認証スキーム”、Ｃｏｍｍ．ＡＣＭ、第１７巻、８号、４３７－４４２頁（１９７４年）である。このＰＳＰは暗号化の形で蓄積できるがその必要は無い。図２にこの銀行のデータベース３へのエントリ２００例を示す。

【００１７】ここで説明の便宜上次のように仮定する。この顧客名はミスタ・デービィッドＢ．スミス、そのロ座番号は“ＸＹＺ”、そのＰＩＮは“１２３４”、およびそのＰＳＰは“家でチャリティが始る”とする。こうするとこの銀行のデータベース３のエントリ２００に下記の入力がある。氏名＝ミスタ・デービィッドＢ．スミス、口座＝ＸＹＺ、ＰＩＮ＝ＯＷ（１２３４）、ＰＳＰ＝家でチャリティが始る、で図２に示す通りである。ここで“ＯＷ（１２３４）”は特定のワンウェイ・ファンクションを用いたＰＩＮの暗号化形である。図３に本発

明の認証法による認証プロセスの流れ図を示し、これを参照し説明を続ける。

【００１８】顧客、ここでは例えば、ミスタ・デービィッドＢ．スミスが、例えば、ＡＴＭ１０の端末を用いて金融トランザクションの実行を所望する場合、ステップ３００に示すようにこの顧客はその銀行カードをそのＡＴＭ１０のスロット１２に挿入する。ステップ３０５において、このＡＴＭはこのカードからその口座情報を読取る。前述のようにこの情報には通常この顧客名のデービィッドＢ．スミスと口座番号のＸＹＺがある。当然のことであるが、この顧客がその端末に端末機読取り可能カードを挿入しないで手動でその端末にその口座情報を入力するようなトランザクション実行システムも可能である。次にステップ３１０において、このＡＴＭ１０は通信回線９でその銀行ホスト２と接触する。ステップ３１５において、このＡＴＭ１０とこの銀行ホスト２は、以下に詳しく説明するツーウェイ・チャレンジレスポンス（ｔｗｏ－ｗａｙ　ｃｈａｌｌｅｎｇｅ－ｒｅｓｐｏｎｓｅ）に参加する。

【００１９】さらに具体的に説明すると、ステップ３２０において、このＡＴＭ１０はこの銀行ホスト２に対し正当であることを確証するようその身元を明らかにするつまり身元認証する。ステップ３４０において、この銀行ホスト２はこのＡＴＭ１０に対しこのＡＴＭ１０は正当な銀行に接触したことを確証するようその身元を明らかにするつまり身元認証する。このＡＴＭと銀行ホスト間に生ずるツーウェイ・チャレンジレスポンスは一方が他方に対しその身元を認証できる限り特定の形に限定するものではない。通信システムにおいて要素を認証する認証方法は既知である。本発明の一実施態様ではこの認証スキームは暗号方式を用いてそれぞれが適切なキーを持つかその正否を決める。特に各要素はその他方がまさにその等しい暗号キーを保持しているかそれを検証する。

【００２０】このような認証スキームの一例に前記米国特許第４、７９９、０６１号に開示のスキームを挙げることができる。銀行ホストが保持するキーとＡＴＭに蓄積されたキーの身元を明らかに検証する身元検証の好ましい実施例を図４に示す。説明の便宜上相互に検証しようとする端末とホストはそれぞれこのＡＴＭ１０とホスト２であると仮定する。さらに説明の便宜上このホストは暗号キーＫ１をこのＡＴＭは暗号キーＫ２を持つと仮定する。当然のことであるが、この銀行とＡＴＭが正当である場合にはこの２個のキーのＫ１とＫ２は等しく、それらはキーＫに等しいと定義する。参照する図４ではステップ３２１に示すようにこのＡＴＭ１０はその通し番号Ｓを銀行ホスト２へ送信する。この情報は暗号形では送信しない。

【００２１】次にステップ３２２において、このホスト２はその乱数ジェネレータ８を用いて第１の乱数ＣＡ を

生成する。次にステップ３２３において、このホスト２はそのＡＴＭ１０へこの乱数ＣＡ を送信する。またこの情報は暗号形で送信する必要はない。ステップ３２５において、このＡＴＭ１０は、そのキーＫ２と暗号論理１７を用いてＳとＣＡ と第１の指示コードの暗号ｅK2（Ｓ、ＣＡ 、０）を計算する。この指示コードは指示ビット“０”で示したが、他の指示コードも同様に使用できる。またステップ３２６において、このＡＴＭ１０はまたその乱数ジネレータ２５を用いて第２の乱数ＣＢ を生成する。次にステップ３２７において示すように、このＡＴＭ１０はＣＢ とそのＳとＣＡ と第１の指示コードの暗号をホスト２に送信する。

【００２２】ステップ３３０において、ただしこのステップ３３０はそのステップ３２５ないし３２７に先だって、またはステップ３２５ないし３２７と同時に、さらにまたはステップ３２５ないし３２７に続いて、のいずれかで生ずることができるステップであるが、このステップ３３０において、このホスト２はそのキーＫ１と暗号論理５を用いてＳとＣＡ と第１の指示コードの暗号ｅK1（Ｓ、ＣＡ 、０）を計算する。次にステップ３３１に示すように、ステップ３２７、３３０に続きこのホスト２はコンパレータ７においてＳとＣＡ とその指示コードのホストの暗号を同じ情報のＡＴＭの暗号と比較する。この暗号値が等しくない場合には、ステップ３３２において、このホスト２はそのＡＴＭ１０との間に設定された通信回線を切断する。またステップ３３５に示すように、このホスト２はそのトランザクション実行システムに不正端末が結合された可能性があることをシステム・オペレータに警告する。

【００２３】これに反しこの暗号値が等しいことをこのホスト２が検証した場合、ステップ３３６で示すように、このＡＴＭ１０は認証される。ステップ３４５において、このホスト２はそのキーＫ１と暗号論理５を用いてＳとＣＢ と第１の指示コードと異なる第２の指示コードの暗号ｅK1（Ｓ、ＣＢ 、１）の計算に進む。次にステップ３４７において、このホスト２はそのＳとＣＢ と第２の指示コードの暗号をそのＡＴＭ１０に送信する。ステップ３５０において、ただしこのステップ３５０はステップ３４５、３４７に先だって、またはステップ３４５、３４７と同時に、さらにまたはステップ３４５、３４７に続いて、のいずれかで生ずることができるステップであるが、このステップ３５０において、このＡＴＭ１０はそのキーＫ２と暗号論理１７を用いてＳとＣＢ と第２の指示コードの暗号ｅK2（Ｓ、ＣＢ 、１）を計算する。

【００２４】次にステップ３５１で示すように、このＡＴＭ１０はそのコンパレータ１９を用いてそのＳとＣＢ と第２の指示コードの暗号を同じ情報のホストの暗号と比較する。この暗号値が等しくない場合には、ステップ３５２において、このＡＴＭ１０はそのホスト２との間

に設定された通信回線を切断する。次にステップ３５３に示すように、そのプレゼンテーション・モジュール２２でエラー・メッセージを表示し、ステップ３５４に示すように、スロット１２を経てその顧客のカードをリターンする。またステップ３５５において、このＡＴＭ１０はそのトランザクション実行システムに不正なホストが結合された可能性があることをシステム・オペレータに警告する。これに反して、その暗号値が等しいことをこのＡＴＭ１０が検証した場合、ステップ３５６に示すように、このホスト２は認証される。

【００２５】このステップ３５６でこの銀行ホスト２とＡＴＭ１０間のツーウェイ・チャレンジレスポンスは完了し、ステップ３５９において示すように、本発明の方法は図３のステップ３６０に続く。ここで付記すべきことは前記ツーウェイ・チャレンジレスポンスには種々の変形が可能である。例えば、ステップ３３０ないし３３１の代りに、ステップ３２７においてこのホスト２はそのＡＴＭ１０から受信した暗号情報をそのキーＫ１と解読論理６を用いて解読し、ＳとＣＡ と第１の指示コードを検索したかそれを検証する。それらが検索された場合には、ステップ３３６において、このホスト２は認証される。同様の変形がこのステップ３５０ないし３５１について可能である。具体的に説明すると、ステップ３４７においてこのＡＴＭ１０はそのホスト２から受信した暗号情報をそのキーＫ２と解読論理１８を用いて解読する。

【００２６】そしてＳとＣＢ と第２の指示コードを検索したかそれを検証する。それらが検索された場合には、ステップ３５６におけるようにこのホスト２は認証される。図３に戻り説明を続ける。ステップ３６０において、このＡＴＭ１０はその口座情報をこの銀行ホスト２へ送信する。このホスト２は、そのデータベース３からこの顧客の口座に対応するエントリ２００に含まれた情報を検索し、ステップ３７０において、このホスト２はそのＡＴＭ１０へこの顧客のＰＳＰ“家でチャリティが始る”を送信する。またここで以下に説明する利用のためそのワンウェイ・ファンクションで暗号化したこの顧客のＰＩＮをそのＡＴＭ１０へ送信できる。次にステップ３８０において、この顧客のＰＳＰを組込んだメッセージを通信してこのＡＴＭ１０はその身元をこの顧客に対し認証する。

【００２７】例えば、このＡＴＭ１０はそのプレゼンテーション・モジュール２２で次のようなメッセージを表示する。例えば、「スミスさん、おはようございます。スミスさんのパーソナル・セキュリティ・フレーズは“家でチャリティが始る”です。これが正しい場合はスミスさんの４桁のパーソナル識別番号を入力してください。」である。この顧客のミスタ・スミスがこのＰＳＰを自分自身のＰＳＰであると認識する場合にのみステップ３９０においてこの顧客のミスタ・スミスは自分のＰ

11

ＩＮをそのキーボード２１に入力する。このＰＳＰが静止画像または画像シーケンスの形である場合、同じようなメッセージはこの顧客とこの英数字ＰＳＰをそのビデオＰＳＰにより代えて通信する。

【００２８】同様に、このＰＳＰが録音音声の形の場合、同じようなメッセージはこの顧客とそのプレゼンテーション・モジュール２２を経て音声で通信された音声ＰＳＰによりこの英数字ＰＳＰを代えて通信する。好ましい実施例では、このＡＴＭ１０とホスト２が相互に認証してしまうと、後続するこれらの間の通信はすべてこれら通信の安全を保障するため暗号形で送信される。このＡＴＮ１０とホスト２は、例えば、その共用キーのＫを用いて継続が可能である。または、このＡＴＭ１０とホスト２は、従来周知の方法でなんらか他の機構によりセッション・キーを取決めたりまたはその回線９の安全を保障したりすることができる。ここでは説明の便宜上このＡＴＭ１０とホスト２はそのキーＫを継続使用すると仮定する。

【００２９】またここで不正ユーザによる応答アタックを回避するためトランザクション識別子を入れる。例えば、このトランザクション識別子はそのステップ３２２またはステップ３２６で生成した乱数のなかの一つを使用することができる。またはなんらか他の適当なトランザクション識別子の使用も可能である。ここでは説明の便宜上このトランザクション識別子として乱数ＣＡ を使用すると仮定する。本発明の好ましい実施例では図５に示すように、ステップ５０１においてこのＡＴＭ１０は暗号論理１７とそのキーＫを用いてこの顧客名とその口座番号とこの乱数ＣＡ を含む口座情報を暗号化し、ステップ５０３において、この暗号化口座情報をそのホスト２へ送信する。

【００３０】この口座情報の暗号形を受信すると、ステップ５０５において、このホスト２は解読論理６とその共用キーＫを用いてこの暗号化口座情報を解読する。図５においてはこの共用キーＫを用いる暗号解読を項ｅＫ-1で表す。次にステップ５０７において、このホスト２はこの顧客の口座に対応するエントリ２００に含まれた口座情報をそのデータベース３から検索する。ステップ５０９において、このホスト２は暗号論理５とその共用キーＫを用いてこの顧客のＰＳＰとＣＡ を暗号化する。次にステップ５１１に示すように、このホスト２はそのＡＴＭ１０へこの暗号化ＰＳＰ情報を送信する。この暗号化ＰＳＰ情報を受信すると、ステップ５１３において、このＡＴＭ１０は解読論理１８を用いてこの暗号化ＰＳＰ情報を解読する。

【００３１】本発明の方法は前記ステップ３８０、３９０に示したように進むが、ここでは便宜上図５においてステップ５１５、５１６で再示した。またこのＡＴＭ１０がこの顧客のＰＳＰをこの顧客に通信してこの顧客に対しその身元を明らかにするつまり身元認証した後のみ

12

この顧客はそのキーボード２１上にこの顧客のＰＩＮを入力する。この顧客がそのＰＩＮを入力してしまうと、このＡＴＭ１０はそのＰＩＮの処理を従来周知の標準的な方法の中のいずれかの方法にしたがって行いユーザを認証する。例えば、このＡＴＭ１０はそのＰＩＮを暗号形でこのホスト２へ送信する。次にこのホストは有効なＰＩＮが入力されたことを検証しこのＡＴＭにこのトランザクションを進めるよう指示する。または、端末１０のような新端末をオンライン状態にすると、この銀行１はまたこれにそのワンウェイ・ファンクションを蓄積する。

【００３２】この状況においては図３のステップ３７０または図５のステップ５１１において、このＰＩＮは、そのワンウェイ・ファンクションで暗号化されて、このＡＴＭ１０へこの顧客のＰＳＰと共に送信される。図３のステップ３９０または図５のステップ５１６において、この顧客がそのＰＩＮを入力してしまうと、このＡＴＭ１０はこれをその内蔵ワンウェイ・ファンクションを用いて暗号化しその結果をこの銀行ホストから受信した値と比較する。それらが等しい場合にはこのＡＴＭ１０はこのトランザクションを進ませる。以上本発明の説明は、一つの銀行を取上げ、この銀行がそれ自身の銀行カードを発行しその銀行ホストに結合する複数のＡＴＭで利用する場合について行ったが、さらに本発明は次のような交換システムでも利用可能である。

【００３３】それは、複数の銀行がそれら自身のそれぞれのＡＴＭにおいてその他の銀行が発行したカードも引受けることを合意した交換システムであり、ここでも本発明は適用可能である。さらに、本発明の以上の説明はＡＴＭで行ったが、他の種類の端末でも本発明は適用可能である。例えば、業者売場の販売時点の端末でこれが顧客つまりユーザに機密情報を入力するよう要求する端末も本発明の適用可能な端末として挙げることができる。さらにまた、以上の説明は、本発明の一実施例に関するもので、この技術分野の当業者であれば、本発明の種々の変形例がさらに考え得るが、それらはいずれも本発明の技術的範囲に包含される。

【００３４】

【発明の効果】以上述べたごとく、本発明の方法では従来法のようにカード形状デバイスにハードウェアの追加など厄介な変更を必要とせずさらに端末を有効に認証して機密データが例えば業者売場の販売時点端末のような端末に不当に保持されることもなく本発明により従来法に比し簡単で有用な対顧客端末認証法がトランザクション実行システムに提供でき安全保障の点で大きく向上する。

【図面の簡単な説明】

【図１】本発明の方法が特に好都合であるようなトランザクション実行システムの例を示すブロック図である。

【図２】本発明の方法のデータベース・エントリ例を示

13　　14

す図である。

【図３】本発明の方法による認証プロセスのステップを示す流れ図である。

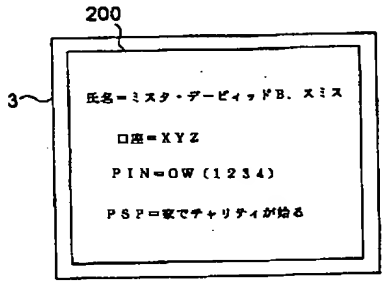
【図４】本発明の方法により相互に端末とホストを認証する好ましい実施例のステップを示す流れ図である。

【図５】本発明の方法により端末とホスト間の通信交換の好ましい実施例のステップを示す流れ図である。

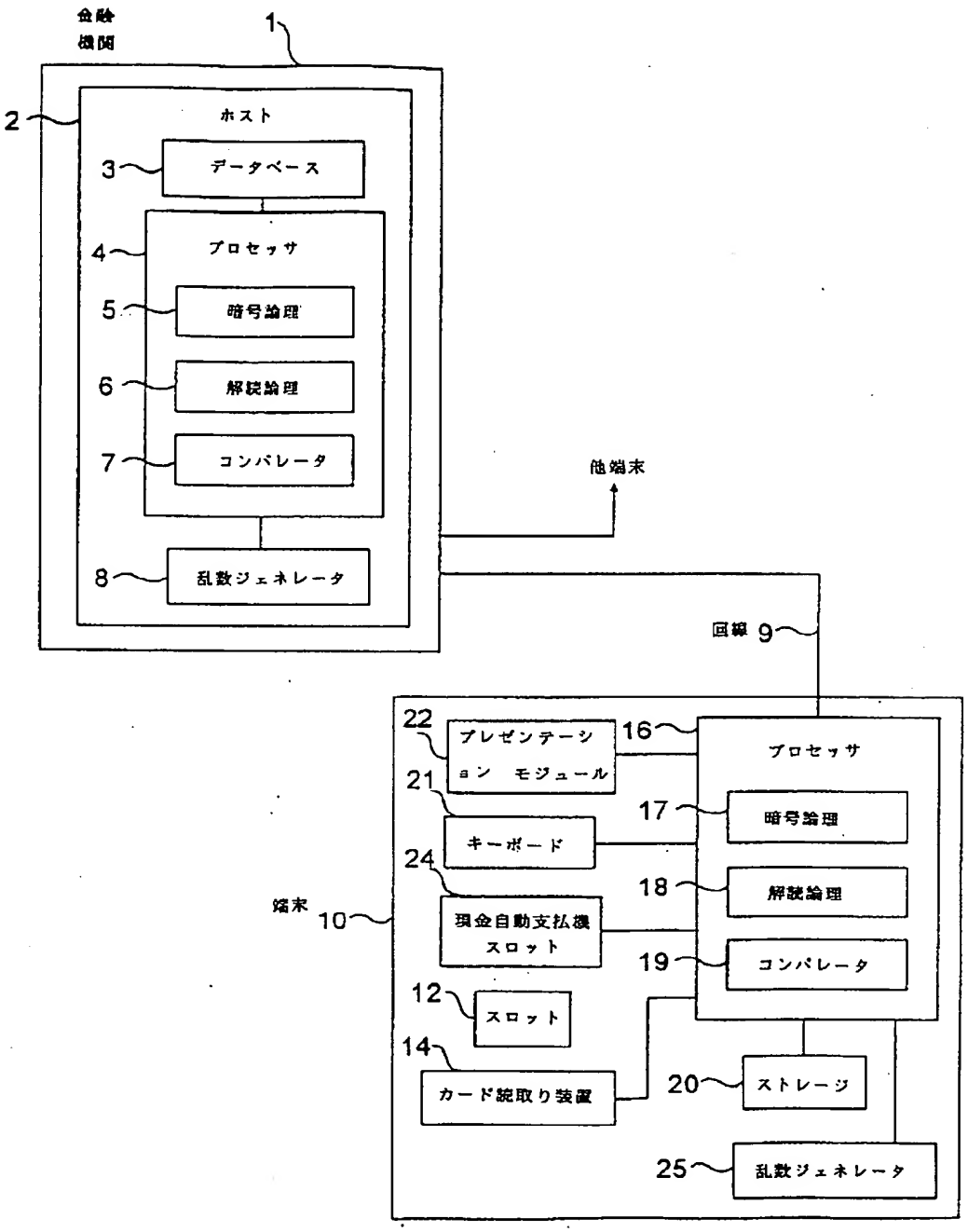
【符号の説明】

１　（金融）機関
２　ホスト
３　データベース
４　プロセッサ
５　暗号論理
６　解読論理
７　コンパレータ
８　乱数ジェネレータ
９　通信回線
１０　端末（自動窓口端末機（ＡＴＭ））
１２　スロット
１４　カード読取り装置
１６　プロセッサ
１７　暗号論理
１８　解読論理
１９　コンパレータ
２０　ストレージ
２１　キーボード
２２　プレゼンテーション・モジュール
２４　スロット（現金自動支払機）
２５　乱数ジェネレータ
２００　データベース・エントリ

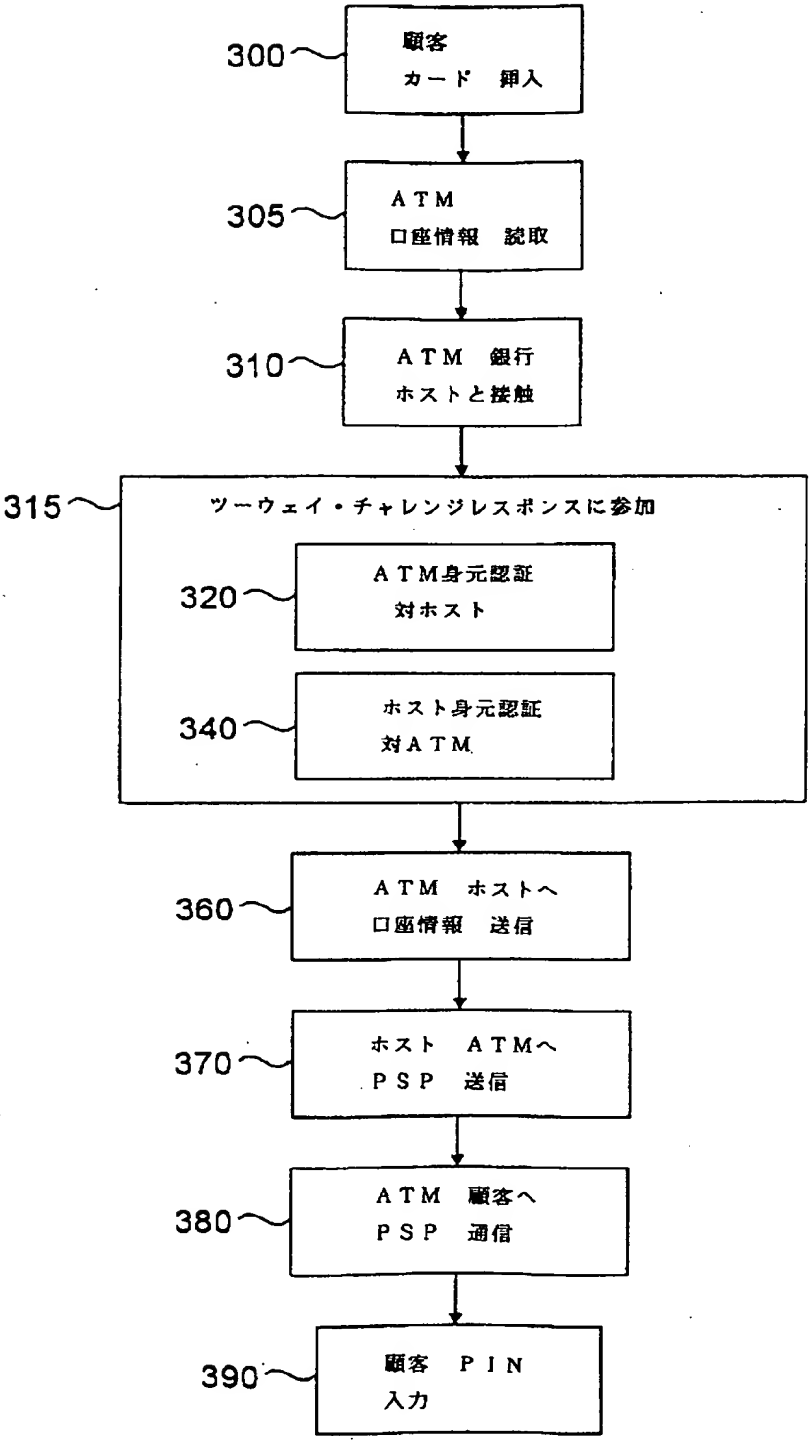
【図２】



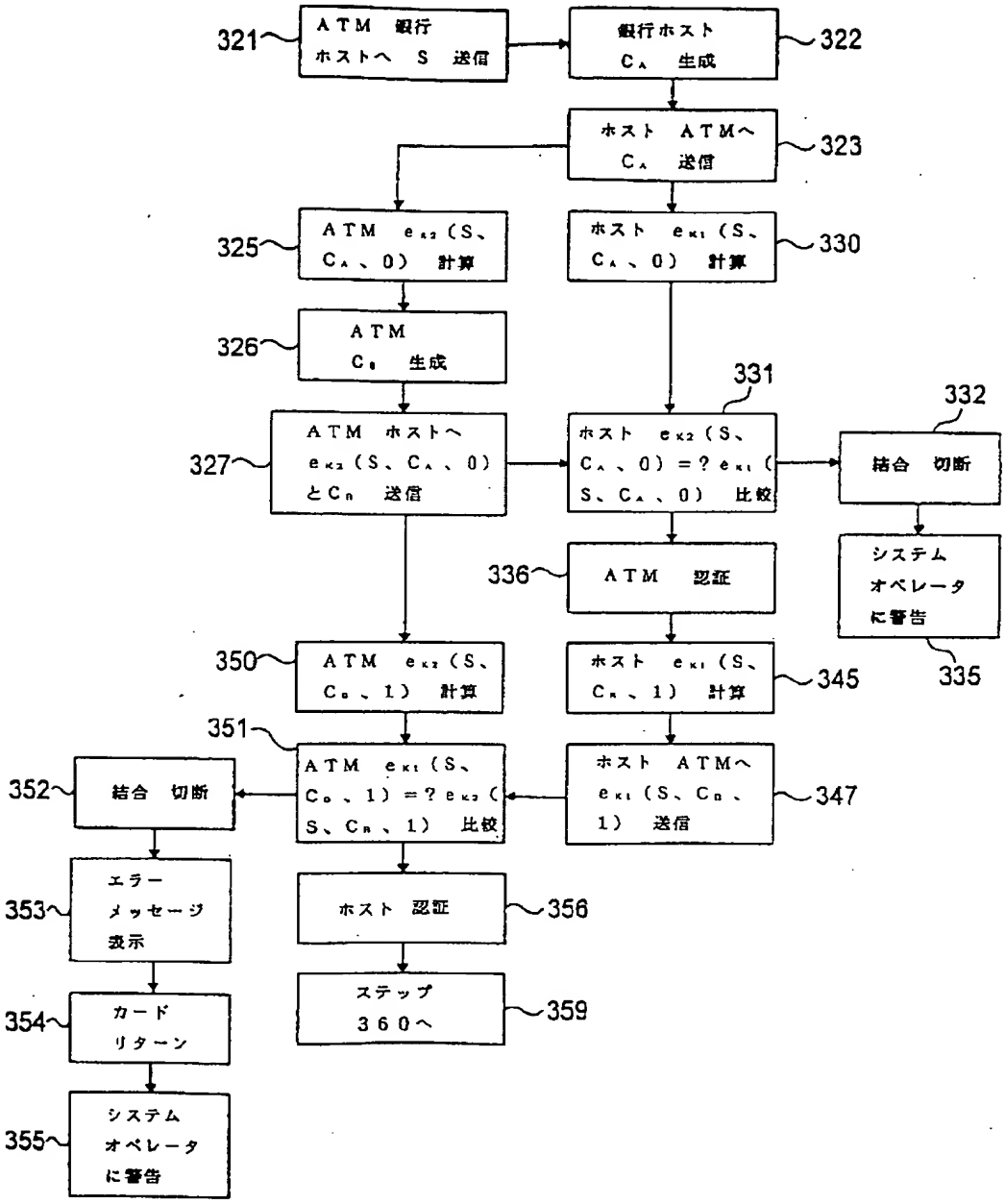
【図１】


金融機関
1
2
ホスト
3
データベース
4
プロセッサ
5
暗号論理
6
解読論理
7
コンパレータ
8
乱数ジェネレータ
他端末
回線 9
端末 10
22
プレゼンテーション モジュール
21
キーボード
24
現金自動支払機スロット
12
スロット
14
カード読取り装置
16
プロセッサ
17
暗号論理
18
解読論理
19
コンパレータ
20
ストレージ
25
乱数ジェネレータ

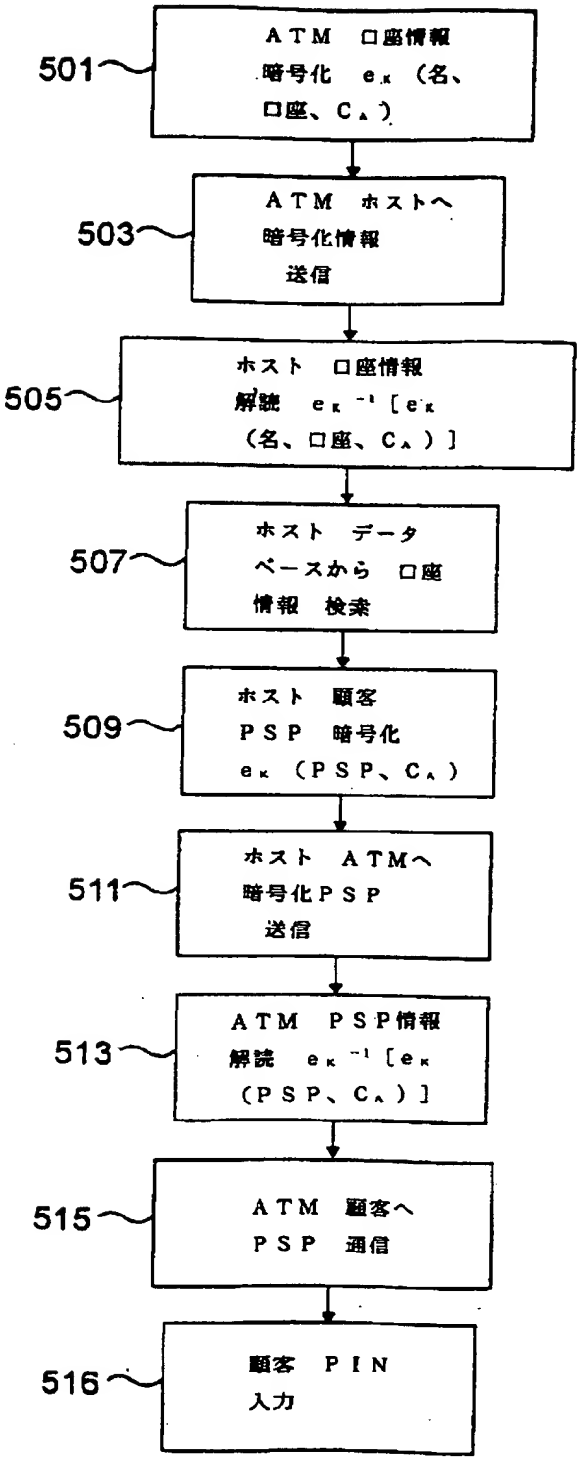
【図３】


300
顧客
カード 挿入
305
ＡＴＭ
口座情報 読取
310
ＡＴＭ 銀行
ホストと接触
315
ツーウェイ・チャレンジレスポンスに参加
320
ＡＴＭ身元認証
対ホスト
340
ホスト身元認証
対ＡＴＭ
360
ＡＴＭ ホストへ
口座情報 送信
370
ホスト ＡＴＭへ
ＰＳＰ 送信
380
ＡＴＭ 顧客へ
ＰＳＰ 通信
390
顧客 ＰＩＮ
入力

【図４】


321
ＡＴＭ　銀行
ホストへ　Ｓ　送信
銀行ホスト
C_A　生成
322
ホスト　ＡＴＭへ
C_A　送信
323
325
ＡＴＭ　e_{k2}（Ｓ、
C_A、０）　計算
ホスト　e_{k1}（Ｓ、
C_A、０）　計算
330
326
ＡＴＭ
C_B　生成
331
332
327
ＡＴＭ　ホストへ
e_{k2}（Ｓ、C_A、０）
とC_B　送信
ホスト　e_{k2}（Ｓ、
C_A、０）＝？e_{k1}（
Ｓ、C_A、０）　比較
結合　切断
システム
オペレータ
に警告
335
336
ＡＴＭ　認証
350
ＡＴＭ　e_{k2}（Ｓ、
C_B、１）　計算
ホスト　e_{k1}（Ｓ、
C_B、１）　計算
345
351
ＡＴＭ　e_{k1}（Ｓ、
C_B、１）＝？e_{k2}（
Ｓ、C_B、１）　比較
ホスト　ＡＴＭへ
e_{k1}（Ｓ、C_B、
１）　送信
347
352
結合　切断
エラー
メッセージ
表示
353
ホスト　認証
356
354
カード
リターン
ステップ
３６０へ
359
355
システム
オペレータ
に警告

【図５】


501
ＡＴＭ　口座情報
暗号化　e_K（名、
口座、C_A）
503
ＡＴＭ　ホストへ
暗号化情報
送信
505
ホスト　口座情報
解読　$e_K^{-1}[e_K$
（名、口座、C_A）]
507
ホスト　データ
ベースから　口座
情報　検索
509
ホスト　顧客
ＰＳＰ　暗号化
e_K（ＰＳＰ、C_A）
511
ホスト　ＡＴＭへ
暗号化ＰＳＰ
送信
513
ＡＴＭ　ＰＳＰ情報
解読　$e_K^{-1}[e_K$
（ＰＳＰ、C_A）]
515
ＡＴＭ　顧客へ
ＰＳＰ　通信
516
顧客　ＰＩＮ
入力

フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	FI		技術表示箇所
H04L 9/10 9/12					
			H04L 9/00	Z	